UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/617,632	07/11/2003	Leonard D. Rarick	5681-64400	4259

35690 7590 02/22/2007		EXAMINER	
MEYERTONS, HOOD, KIVLIN, KOWERT & GOETZEL, P.C.		DINH, MINH	
700 LAVACA, SUITE 800			
AUSTIN, TX 78701		ART UNIT	PAPER NUMBER
		2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

	Application No.	Applicant(s)
Office Action Summary	10/617,632	RARICK ET AL.
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>24 November 2006</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-49</u> is/are pending in the application.

    4a) Of the above claim(s) <u>14-18,34-37 and 41-49</u> is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-13,19-33 and 38-40</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>11 July 2003</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date <u>12/3/04; 12/13/04</u>.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____ .

DETAILED ACTION

1.   Claims 1-13, 19-33 and 38-40 have been examined.

Election/Restrictions

2.   Applicant's election without traverse of species (i) in the reply filed on

11/24/06 is acknowledged. However, Applicant fails to elect, within species

(i), either species (ia) or (ib) in the reply. During a telephone conversation

with Erik Heter on 02/09/07 a provisional election was made without

traverse to prosecute species (ia) corresponding to claims 1-13, 19-33 and

38-40. Affirmation of this election must be made by applicant in replying to

this Office action. Claims 14-18, 34-37 and 41-49 are withdrawn from

further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a

non-elected invention.

3.   Applicant is reminded that upon the cancellation of claims to a non-

elected invention, the inventorship must be amended in compliance with 37

CFR 1.48(b) if one or more of the currently named inventors is no longer an

inventor of at least one claim remaining in the application. Any amendment

of inventorship must be accompanied by a request under 37 CFR 1.48(b)

and by the fee required under 37 CFR 1.17(i).

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis

for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or
> described as set forth in section 102 of this title, if the differences between the subject
> matter sought to be patented and the prior art are such that the subject matter as a
> whole would have been obvious at the time the invention was made to a person having
> ordinary skill in the art to which said subject matter pertains. Patentability shall not be
> negatived by the manner in which the invention was made.

5.   Claims 1-9, 11-13, 19-30, 32-33 and 38-40 are rejected under 35

U.S.C. 103(a) as being unpatentable over Matthews, JR. (2003/0044007)

(hereinafter "Matthews").

        Regarding claims 1, 3-8, 19-22, 24-29 and 38-40, Mathews discloses a

method for improving ARC4 encryption processing using pipelining wherein

the pipelining includes a stage for obtaining a value A (i.e., Si) from an array

having a plurality of values (fig. 5, step 503; paragraph 0050); a stage for

determining a value B (i.e., Sj) based on the value A (fig. 5, step 507;

paragraph 0050); a stage for obtaining a value V (i.e., St) from a position in

the array that is based on the value A and the value B (fig. 5, step 515;

paragraph 0050); and exclusive-ORing the value V with a data value that

forms a portion of the information (paragraph 0027).

        Matthews does not disclose that the exclusive-Oring step is part of the

pipeline. It would have been obvious to one of ordinary in the art at the

time of the invention was made to make the exclusive-Oring step a part of

the pipeline (i.e., an additional stage) to increase the system throughput.
The more stages there are in a pipeline, the more a system can produce in a
given amount of time.

Matthews discloses that each step is performed in a separate pipeline
stage. Matthews does not disclose that the first two steps are performed in
a first pipeline stage, and the last two steps are performed in a second
pipeline stage. The number of stages in a pipeline is determined based on
the hardware structure of the component processing the pipeline (i.e.,
because pipeline stages in a pipeline are executed concurrently, there must
be at least one hardware processing unit for each pipeline stage).
Therefore, combining four pipeline stages into two pipeline stages would be
merely a matter of obvious engineering choice. It would have been obvious
to combine four pipeline stages into two pipeline stages if the hardware
structure could only support two concurrent operations at a time.

Regarding claims 2 and 23, Matthews further discloses that the array
is initialized using an encryption key sequence (fig. 4; paragraph 0035).

Regarding claims 9, 11-13, 30 and 32-33, Matthews further discloses
that each of the plurality of values is stored in a storage location comprising
flip-flops (fig. 6, paragraph 0048).

6.   Claims 10 and 31 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Matthews as applied to claims 9 and 30 above, and

further in view of Lai et al. (5,485,619). Matthews discloses incrementing

array index [i] each iteration to obtain value A (Si) from the array (the S-

box). Matthews does not disclose shifting the array each iteration. Lai

discloses that iterative computations (DO-loop), which involve incrementing

an array index, are implemented by shifting the array each iteration (3col.

14, lines 11-21). It would have been obvious to one of ordinary in the art at

the time the invention was made to modify Matthews method to shift the

array each iteration, as taught by Lai, in order to eliminate processing and

storage inefficiencies of compiled array functions (col. 10, line 60 – col. 11,

line 9).

Conclusion

7.   The prior art made of record and not relied upon is considered

pertinent to applicant's disclosure.

U.S. Patent No. 6,549,622 to Matthews, JR.

U.S. Patent No. 6,980,649 to Batcher

U.S. Patent No. 7,043,017 to Swindlehurst et al.

Hamalainen et al., "Hardware Implementation of the Improved WEP

And RC4 Encryption Algorithms for Wireless Terminals"

Mano, "Computer System Architecture"

Mano et al., "Logic and Computer Design Fundamentals"

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained

from the Patent Application Information Retrieval (PAIR) system. Status

information for published applications may be obtained from either Private

PAIR or Public PAIR. Status information for unpublished applications is

available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on

access to the Private PAIR system, contact the Electronic Business Center

(EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-

1000.

MD

Minh Dinh
Examiner
Art Unit 2132

2/13/07

Benjamin E. Lanier
Examiner AU 2132